Application No. 39378/15

IN THE EUROPEAN COURT OF HUMAN RIGHTS
BETWEEN:

STANDARD VERLAGSGESELLSCHAFT MbH

Applicant

-and-

AUSTRIA

Respondent

WRITTEN COMMENTS OF THE MEDIA LEGAL DEFENCE INITIATIVE THIRD PARTY INTERVENER[1]

Introduction

1. The right to freedom of expression and the right to privacy are fundamental to an individual's ability to communicate freely. In particular, an individual's right to communicate freely can be greatly enhanced by the ability to do so anonymously or pseudonymously. This case provides an important opportunity for the Court to set out the relevant principles underlying the right to communicate anonymously online, and the factors that should be taken into account when determining whether and to what extent a measure compelling internet service providers to disclose the data of internet users can be compatible with Article 10 of the European Convention on Human Rights.

2. Anonymity provides individuals with the conditions necessary to fully exercise their right to freedom of expression. For instance, it provides individuals with the ability to communicate without fear of the reprisals that might result from their identification. These reprisals might take the form of arrest, detention, or prosecution by state authorities, or threats of litigation, or even violence, from non-state actors. A further consequence of the loss of anonymity might include social exclusion by family or friends, or the loss of a job or denial of advancement by an employer. Accordingly, the disinhibiting effect of anonymity can advance discussion on matters of public interest, and promote an individual's autonomy and self-determination.

3. This intervention provides an analysis of comparative and international law to address the following principles relevant to the circumstances under which identifying data of an anonymous user may be justifiably disclosed in accordance with the European Convention on Human Rights (the 'Convention'):

   (i) The right to freedom of expression under Article 10 of the Convention protects anonymous speech online;

   (ii) An internet service provider should only be required to disclose user data by a court order; and

   (iii) A court should only order an internet service provider to disclose user data where certain minimum standards are met, including a demonstration that there is a *prima facie* cause of

[1] The Media Legal Defence Initiative (the 'Intervener') submits these written comments pursuant to leave granted by the President of the Fifth Section under Rule 44 §3 of the Rules of the Court and as set out in the letter dated 4 September 2017 from the Fifth Section Registrar, C. Westerdiek.

action against the user, and that the user had been afforded an opportunity to challenge the request for disclosure.

Article 10 of the Convention protects anonymous expression online

4. The internet has provided and facilitated individuals with the means of disseminating and receiving information and ideas instantaneously, on a global scale, and at a relatively low cost.[2] The Court has recognised that the internet has become one of the primary and principal means for individuals to exercise their right to freedom of expression.[3] The right to freedom of expression online, as guaranteed by Article 10 of the Convention, must be interpreted to include the right to receive and impart information and ideas anonymously. In *Delfi v. Estonia*, the Grand Chamber recognised the different degrees of anonymity that are possible on the Internet[4] and implied that online anonymity is to be protected under the Convention. In its judgment, the Grand Chamber reasoned that;

> "[a]lthough freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others"[5]

5. In 2003, the Council of Europe Committee of Ministers adopted the *Declaration on freedom of communication on the Internet* which recognised the importance of protecting anonymous expression under the Convention. By adopting the Declaration, the Member States of the Council of Europe declared that they seek to abide by the principle that they should "respect the will of users of the Internet not to disclose their identity".[6] The Committee of Ministers explained that the principle had two aspects to it;

> "Firstly, users may have a valid reason not to reveal their identity when they have statements published on the Internet. Obliging them to do so could restrict excessively their freedom of expression. It would also deprive society of potentially valuable information and ideas.
>
> Secondly, users need protection against unwarranted on-line surveillance by public or private entities. Member States should therefore, for example, allow the use of anonymity tools or software which enable users to protect themselves."[7]

6. Under International Law, Article 19 of the International Covenant on Civil and Political Rights (ICCPR) protects the right to freedom of expression in similar terms to Article 10 of the Convention. During the drafting of the ICCPR, an amendment was proposed to prohibit anonymity under Article 19 ICCPR which was objected to on the grounds, among others, that anonymity might at times be necessary to protect the author and that such a clause might prevent the use of pen names.[8] The amendment was later withdrawn.[9] This would suggest that it was the intention of the drafters of the ICCPR to protect anonymous speech under the right to freedom of expression.

---

2 UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and African Commission Special Rapporteur on Freedom of Expression and Access to Information, *Joint declaration on freedom of expression and the Internet*, 1 June 2011.

3 See European Court of Human Rights, *Ahmet Yildirim v. Turkey*, Application No. 3111/10 (2012), par. 54.

4 European Court of Human Rights, *Delfi AS v. Estonia* [GC], Application No. 64569/09 (2015), par. 148.

5 *Id*., par. 149. Citing European Court of Human Rights, *K.U. v. Finland*, Application No. 2872/02, par. 49.

6 Committee of Ministers of the Council of European, *Declaration on freedom of communication on the Internet*, adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies, Principle 7.

7 *Id*., Explanatory Memorandum.

8 United Nations General Assembly, *Draft International Covenants on Human Rights: Report of the Third Committee*, U.N. Doc. A/5000 (5 December 1961), p. 5.

9 *Id*., p. 9.

7. More recently, in 2013, the United Nations General Assembly passed Resolution 68/167, which reaffirmed that the right to privacy is "important for the realisation of the right to freedom of expression and to hold opinions without interference".[10] The reports of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression have expanded on this to recognise the crucial benefit of anonymity on the Internet to the exercise of the right to freedom of expression. In 2011, he observed that;

> "throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously. The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums."[11]

8. In his 2015 report, the United Nations Special Rapporteur referred to the central role of anonymity in "advancing privacy, free expression, political accountability, public participation and debate."[12] He clarified that any restriction on anonymity must meet the test under Article 19 ICCPR that it should be provided for by law, imposed for legitimate grounds, and conform to the strict tests of necessity and proportionality.[13]

9. The approach adopted in Germany in relation this issue is instructive of the importance of anonymity to the right to freedom of expression online. In Germany, anonymous use of the internet is given statutory protection under the Telemedia Act 2007 (*Telemediengesetz*). Furthermore, section 13(6) of the Telemedia Act places a statutory obligation on electronic communications service providers to enable the use of "telemedia" (e.g. websites, email providers, and other internet service providers) anonymously or via a pseudonym where it is technically possible and reasonable. The protections afforded to anonymous speech online were considered by the Federal Supreme Court of Germany (*Bundesgerichtshof*) in the *Spickmich case*, which concerned a teacher who wanted her name and details of her school removed from a social media site that provided pupils with a platform to evaluate their teachers and schools anonymously. Users registered with the website by providing their name and email address, and details of the relevant school. The Federal Supreme Court dismissed the teacher's complaint, reasoning that anonymity was inherent in the use of the Internet and protected by the Telemedia Act. The Federal Supreme Court also added that the obligation to identify an individual with the expression of a particular view would generally, as well as in the school context, lead to self-censorship from fear of the negative consequences of identification. Therefore, the imposition of such an obligation would be incompatible with freedom of expression under Article 5(I) of the German basic law.

10. An early iteration on the protections to be afforded to anonymous speech under the First Amendment can be found in the case of *McIntyre v. Ohio* before the Supreme Court of the United States of America.[14] The principles adopted in that case are worth noting. The case concerned an individual who was distributing leaflets about a proposed school tax levy containing the views of

---

[10] United Nations General Assembly, *Resolution 68/167 on the right to privacy in the digital age*, U.N. Doc. A/RES/68/167 (18 December 2013).

[11] United Nations Special Rapporteur on Freedom of Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N.Doc. A/HRC/17/27 (16 May 2011), par. 53

[12] United Nations Special Rapporteur on Freedom of Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N.Doc. A/HRC/29/32 (22 May 2015), par. 47.

[13] *Id*., par. 31.

[14] Supreme Court of the United States of America, *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

anonymous individuals referred to as "Concerned Parents and Tax Payers". She was told that, in Ohio, it was a violation of State law to write, print or distribute campaigning literature without indicating the name and residence of the person responsible for it, and was subsequently fined. The majority judgment of Stevens J recognised two justifications for protecting anonymous speakers under the First Amendment. First, "[a]nonymity is a shield from the tyranny of the majority".[15] In short, without anonymity, some valuable speech would not be published. Second, "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment".[16]

An internet service provider should only be required to disclose user data by a court order

11. This Court has recognised that an interference with the right to freedom of expression cannot be justified under Article 10 of the Convention if it is not "prescribed by law". This Court has further clarified that an interference will not be "prescribed by law" simply because it has some basis in domestic law.[17] Instead, the relevant domestic law should "be both adequately accessible and foreseeable" while complying with the rule of law.[18] In this regard, the Court has also warned that domestic law must offer "legal protection against arbitrary interferences by public authorities with the rights safeguarded by the Convention."[19] In 2017, the United Nations Special Rapporteur noted that provisions empowering authorities to request user data usually allow such requests to be made based on mere assertions as to the purpose of the data, for example the assertion of national security. He went on to observe that one of the consequences of this approach, in practice, was that anonymous users were "unable to predict with reasonable certainty the circumstances under which their communications and associated data may be disclosed to authorities."[20]

12. The intervener submits that measures compelling internet service providers to disclose the data of anonymous users will not be "prescribed by law" unless legal protections are in place to protect users against arbitrary abuse. The intervener further submits that such legal protection can only be offered where such measures are formally ordered by a court. This Court, in *Delfi v. Estonia*, noted that "[t]he release of [identifying data of anonymous users] would *usually* require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions."[21] This can be contrasted with the position of the United Nations Special Rapporteur on Freedom of Opinion and Expression, who has clearly stated that internet service providers "should only be compelled to release user data when ordered by judicial authorities certifying necessity and proportionality to achieve a legitimate objective."[22] The intervener submits that the latter approach is more closely aligned to the Court's previous jurisprudence with regard to the protection of journalistic sources and surveillance, which raise similar implications for freedom of expression as the disclosure of anonymous user data.

---

15 *Id*., p. 357.
16 *Id*., p. 342.
17 See European Court of Human Rights, *Sanoma Uitgevers B.V. v. the Netherlands* [GC], Application No. 38224/03 (2010), par. 81.
18 *Id*., par. 81 and 82.
19 *Id*., par. 82.
20 UN Special Rapporteur, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N.Doc. A/HRC/35/22 (30 March 2017), par. 18.
21 European Court of Human Rights, *Delfi AS v. Estonia* [GC], Application No. 64569/09 (2015), par. 148. [Emphasis added]
22 United Nations Special Rapporteur on Freedom of Expression, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N.Doc. A/HRC/35/22 (30 March 2017), par. 19

13. The disclosure of journalistic sources and surveillance can have negative consequences for the right to freedom of expression due to a breach of an individual's confidentiality in their communications. This is the same for cases concerning the disclosure of anonymous user data. Once confidentiality is undermined, it cannot be restored. It is, therefore, of utmost importance that measures that undermine confidentiality are not taken arbitrarily. This Court has highlighted the need for effective independent review of measures that could undermine the protection of journalistic sources or could subject an individual to surveillance.[23] In *Sanoma Uitgevers v. The Netherlands*,[24] the Grand Chamber held that a particularly important safeguard against arbitrary abuse in cases concerning the protection of journalistic sources is the "guarantee of review by a judge or other independent and impartial decision-making body."[25] The Grand Chamber found that the independent review should ideally take place prior to the handing over of the relevant material. However, the Grand Chamber also noted that it may not always be possible for prosecuting authorities to make detailed applications to the courts in urgent cases. It reasoned that, in such instances;

> "an independent review carried out at the very least prior to the access and use of obtained materials should be sufficient to determine whether any issue of confidentiality arises, and if so, whether in the particular circumstances of the case the public interest invoked by the investigating or prosecuting authorities outweighs the general public interest of source protection. It is clear, in the Court's view, that the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality."[26]

14. In light of the interests at stake with the disclosure of anonymous user data, the Intervener submits that user data should only be disclosed pursuant to a court order, and following a review by a court of whether the public interest favours the disclosure of such data. It should not be left to a third party, such as an internet service provider or an individual seeking the disclosure, to determine whether the data should be disclosed, as such a process would be liable to arbitrary abuse and would insufficiently protect the Convention rights of anonymous users.

A court should only order an internet service provider to disclose user data where certain minimum standards are met

15. Court orders requiring the disclosure of anonymous user data, particularly a user's identity, must meet the test of necessity and proportionality. Case law from a number of jurisdictions are instructive on the factors that may be considered before granting such an order to ensure it is both necessary and proportionate.

The applicant must demonstrate to a sufficient degree that a wrongful act has been committed against them, and that the information is sought to enable them to seek redress for that wrongful act

16. In England and Wales, the procedure for obtaining a court order for the disclosure of the identity of an unknown individual was first established in the House of Lords case of *Norwich Pharmacal Co*

---

23 See, for example, European Court of Human Rights, *Roman Zakharov v. Russia* [GC], Application No. 47143/06 (2015); European Court of Human Rights, *Sanoma Uitgevers B.V. v. the Netherlands* [GC], Application No. 38224/03 (2010).

24 European Court of Human Rights, *Sanoma Uitgevers B.V. v. the Netherlands* [GC], Application No. 38224/03 (2010). [Emphasis added]

25 *Id*., par. 90.

26 *Id*., par. 91.

v. Customs and Excise Comrs.[27] Although *Norwich Pharmacal* orders are at the discretion of the courts, the courts can only make such orders once they are satisfied that, *inter alia*, there has been a wrong carried out, or arguably carried out, by an ultimate wrongdoer, and the applicant has shown that the disclosure is for the purpose of obtaining redress for the wrongdoing.[28] The "wrong" may be a crime, tort, breach of contract, equitable wrong, or contempt of court. Therefore, in order to obtain the disclosure of the identity of an anonymous speaker, there must be an "arguable case" that a wrong has been carried out, and it is for the applicant seeking the order to identify this wrong.[29] Subsequent case law from the English courts has clarified that, in exercising their discretion to grant an order for disclosure, the courts will also have regard to "the strength of the claimant's *prima facie* case against the wrongdoer".[30] These requirements ensure that the disclosure is being made for a legitimate purpose, rather than being frivolous, vexatious, or for some ulterior motive.[31]

17. Similarly, in the Netherlands, one of the threshold requirements that needs to be met before a court can order an internet service provider to disclose the identity of its users is that it must be "sufficiently plausible" that the information published by the user is wrongful and harmful.[32] Another requirement is that the individual seeking the identity of the user must have a concrete interest in obtaining the identity of the user.[33] In Ireland, the *Norwich Pharmacal* principles are adopted when determining whether to make an order to disclose the identity of anonymous wrongdoers. This includes a requirement on the plaintiff to present "very clear proof of wrongdoing".[34]

18. In Canada, the identity of an anonymous user can only be sought through a *Norwich Pharmacal* order or through disclosure orders that are made pursuant to provincial rules of civil procedure. A *Norwich Pharmacal* order in the Canadian context will only be granted where a number of threshold requirements are met, including that the applicant must provide evidence sufficient to raise a valid, *bona fide* or reasonable claim.[35] Obtaining a disclosure of user data through provincial civil procedure rules, on the other hand, requires that the applicant establish "a *prima facie* case against the unknown alleged wrongdoer and [that the applicant] is acting in good faith".[36] In *Warman v. Fournier*, the Ontario Superior Court of Justice highlighted the importance of having threshold requirements on the merits of a case when anonymous user data is being sought through a court order. It reasoned that;

> "[i]f disclosure were automatic, a plaintiff with no legitimate claim could misuse the *Rules of Civil Procedure* by commencing an unmeritious action for the sole purpose of revealing the identity of anonymous Internet commentators, with a view to stifling such commentators and

---

27 House of Lords, *Norwich Pharmacal Co. & Others v. Customs and Excise Commissioners*, [1974] AC 133. This case has been followed and expressly referred to in other jurisdictions.

28 Supreme Court of the United Kingdom, *Rugby Football Union v. Viagogo Ltd*, [2012] UKSC 55 (21 November 2012), par. 14 and 15. It is also a requirement before a *Norwich Pharmacal* order may be ordered that the person against whom the order is sought must (a) be mixed up in the wrongdoing so as to have facilitated it; and (b) be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued. See High Court of England and Wales, *Mitsui & Co Ltd v. Nexen Petroleum UK Ltd*, [2005] EWHC 625 (Ch) (29 April 2005), par. 21.

29 House of Lords, *Ashworth Hospital Authority v. MGN Limited*, [2002] 1 WLR 2033, par. 60

30 High Court of England and Wales, *Totalise plc v. The Motley Fool*, [2001] IP & T 764, par. 27

31 See High Court of England and Wales, *Sheffield Wednesday FC & ors v. Hargreaves*, [2007] EWHC 2375 (QB) (18 October 2007), par. 17.

32 Supreme Court of the Netherlands, *Lycos Netherlands B.V/Pessers*, C04/234HR (25 November 2005).

33 *Id*.

34 Supreme Court of Ireland, *Megaleasing Holdings Limited and Quantum Data SA v. Vincent Barrett and Ors*, [1993] ILRM 497.

35 Court of Appeal for Ontario, *GEA Group AG v. Ventra Group Co. et al*., 96 O.R. (3d) 481, par. 49.

36 Ontario Superior Court of Justice (Divisional Court), *Warman v. Fournier et al.*, [2010] ONSC 2126, par. 34.

> deterring others from speaking out on controversial issues. For this reason, the commencement of a defamation claim does not trump freedom of expression or the right to privacy."[37]

19. In cases of defamation, the Ontario Superior Court of Justice noted that the *prima facie* threshold is the most appropriate for two key reasons. First, there is no need for an internet service provider to disclose the data of the anonymous user for the applicant to make out their cause of action in defamation against the wrongdoer.[38] This is because the applicant will know the details of precisely what was done by the unknown defendant. Second, a more robust standard is necessary;

> "to address the chilling effect on freedom of expression that will result from disclosure […] The requirement to demonstrate a *prima facie* case of defamation furthers the objective of establishing an appropriate balance between the public interest in favour of disclosure and legitimate interests of privacy and freedom of expression."[39]

20. In the United States of America, the leading cases of *Dendrite Int'l Inc. v. Doe*[40] and *Doe v. Cahill*[41] establish the standard of review required when a litigant seeks civil discovery to identify an anonymous speaker. Before discovery can be ordered, both cases require that the plaintiff produce sufficient evidence to establish a *prima facie* case on all elements of their claim. These two cases recognise that compelling the disclosure of the identity of an anonymous speaker without first evaluating the merits of the plaintiff's claims fails to sufficiently protect the right to freedom of expression and privacy. Without such a requirement, anonymous critics may be exposed to plaintiffs using discovery to harass, intimidate or silence them. This was addressed in *Doe v. Cahill*, where the Supreme Court of Delaware noted the risk of plaintiffs in defamation cases bringing suits merely to unmask anonymous speakers. It went on to state that it was;

> "concerned that setting the standard too low will chill potential posters from exercising their First Amendment right to speak anonymously. The possibility of losing anonymity in a future lawsuit could intimidate anonymous posters into self-censoring their comments or simply not commenting at all. A defamation plaintiff, particularly a public figure, obtains a very important form of relief by unmasking the identity of his anonymous critics. The revelation of identity of an anonymous speaker may subject [that speaker] to ostracism for expressing unpopular ideas, invite retaliation from those who oppose her ideas or from those whom she criticizes, or simply give unwanted exposure to her mental processes. Plaintiffs can often initially plead sufficient facts to meet the good faith test applied by the Superior Court, even if the defamation claim is not very strong, or worse, if they do not intend to pursue the defamation action to a final decision. After obtaining the identity of an anonymous critic through the compulsory discovery process, a defamation plaintiff who either loses on the merits or fails to pursue a lawsuit is still

---

37 *Id*., par. 33
38 *Id*., par. 41.
39 *Id*., par. 42
40 New Jersey Superior Court, *Dendrite Int'l Inc. v. Doe*, 342 NJ Super 134; 775 A2d 756 (NJ App, 2001). Adopted by appellate courts in Arizona (*Mobilisa Inc v. Doe*, 217 Ariz. 103; 170 P3d 712 (App, 2007)), Indiana (*In re Independent Newspapers v. Junior Achievement of Central Indiana Inc.*, 963 NE2d 534 (Ind. App, 2012)), Maryland (*Independent Newspapers Inc. v. Brodie*, 407 Md 415, 966 A2d 432 (App, 2009)), New Hampshire (*Mtg Specialists Inc. v. Implode-Explode Heavy Indus Inc.*, 160 NH 227, 999 A2d 184 (2010)), Pennsylvania (*Pilchesky v. Gatelli*, 2011 Pa Super 3, 12 A3d 430 (2011)).
41 Delaware Supreme Court, *Doe v. Cahill*, 884 A2d 451 (Del, 2005). Adopted by appellate courts in Kentucky (*Doe v. Coleman*, 436 SW3d 207 (Ky App, 2014)), California (*Krinsky v. Doe*, 159 Cal App 4th 1154; 72 Cal Rptr 3d 231 (2008)), District of Columbia (*Solers Inc. v. Doe*, 977 A2d 941 (DC App. 2009)), Texas (*In re Does 1-10*, 242 SW3d 805 (Tex App, 2007)).

> free to engage in extra-judicial self-help remedies; more bluntly, the plaintiff can simply seek revenge or retribution.[42]

The anonymous user has been notified, and has had an opportunity to respond to the application

21. As the disclosure of an anonymous user's identity engages that user's right to communicate anonymously, it is imperative that the user be afforded an opportunity to put forward his or her case in defence of the alleged wrong and against having their identity disclosed. This is particularly important because internet service providers may not have sufficient interest or knowledge to defend against an application for disclosure of a user's identity. In the United States of America, an attempt to notify an anonymous user forms part of the guidelines set out by *Dendrite Int'l Inc. v. Doe*[43] and *Doe v. Cahill*[44] for civil discovery of the identity of anonymous users. In *Doe v. Cahill*, the Supreme Court of Delaware explained that;

> "[t]he notification provision imposes very little burden on a defamation plaintiff while at the same time giving an anonymous defendant the opportunity to respond. When First Amendment interests are at stake we disfavor *ex parte* discovery requests that afford the plaintiff the important form of relief that comes from unmasking an anonymous defendant."[45]

22. Similar reasoning can be found in the case law of Canada, and England and Wales. For instance, the Court of Appeal of England and Wales has recognised that;

> "[i]t is difficult to see how the court can carry out [the balancing of interests] if what it is refereeing is a contest between two parties, neither of whom is the person most concerned, the data subject; one of whom is the data subject's prospective antagonist; and the other of whom knows the data subject's identity, has undertaken to keep it confidential so far as the law permits, and would like to get out of the cross-fire as rapidly and as cheaply as possible. However the website operator can, where appropriate, tell the user what is going on and to offer to pass on in writing to the claimant and the court any worthwhile reason the user wants to put forward for not having his or her identity disclosed. Further, the court could require that to be done before making an order."[46]

23. Relying on this reasoning, the Canadian courts have observed that anonymous users may have "compelling reasons to remain anonymous that are not immediately obvious, such as a risk to personal safety, and such grounds could not be put before the court absent notice."[47] In a recent case in Ireland, the High Court found that an anonymous user located in Uganda, who was responsible for publishing allegedly defamatory statements, could face a serious threat to his personal safety if his identity was to be disclosed. The High Court refused the application for a *Norwich Pharmacal* order and asked the internet service provider to notify the user that a fresh application could be made if the impugned statements were not removed.[48]

---

42 Delaware Supreme Court, *Doe v. Cahill*, 884 A2d 451 (Del, 2005), p. 457. [Citations removed]
43 New Jersey Superior Court, *Dendrite Int'l Inc. v. Doe*, 342 NJ Super 134; 775 A2d 756 (NJ App, 2001).
44 Delaware Supreme Court, *Doe v. Cahill*, 884 A2d 451 (Del, 2005).
45 *Id*., p. 461.
46 Court of Appeal for England and Wales, *Totalise Plc v Motley Fool Ltd & Anor*, [2001] EWCA Civ 1897 (19 December 2001), par. 26.
47 Ontario Superior Court of Justice (Divisional Court), *Warman v. Fournier et al.*, [2010] ONSC 2126, par. 43; Supreme Court of Nova Scotia, *Olsen v. Facebook Inc.*, 2016 NSSC 155 (17 June 2016), par. 12 to 15.
48 High Court of Ireland, *Muwema v. Facebook Ireland Ltd (No 2)*, [2017] IEHC 69 (8 February 2017), par. 41.

There is no less restrictive means of obtaining the information sought

24. Given the negative consequences that can flow from an internet service provider disclosing the identity of anonymous users, courts should take into account whether there is an alternative means of obtaining the user's identity that would be less restrictive on the right to freedom of expression online.[49] In England and Wales, courts will consider whether the information sought through a *Norwich Pharmacal* order could be obtained from another source when exercising its discretion to make such an order.[50] In the Netherlands, when deciding whether internet service providers should disclose the names and addresses of website holders, courts have taken into account whether no other "less far-reaching option" could be considered in order to retrieve the information sought.[51] In Canada, when deciding whether a *Norwich Pharmacal* order is to be granted, courts must be satisfied that "the third party is the only practicable source of the information available".[52] In Canadian cases whether disclosure is sought through civil procedure rules, courts will only compel third-party disclosure of the identity of an anonymous user where the person seeking the order has "taken reasonable steps to identify the anonymous party and has been unable to do so".[53]

The applicant's interest in disclosure has been sufficiently balanced against the rights to freedom of expression and privacy

25. When determining whether the disclosure of the identity of an anonymous user is necessary and proportionate, a court must ensure that the applicant's interest in disclosure and seeking redress for an alleged wrongdoing has been sufficiently balanced against (i) the anonymous user's right to freedom of expression and privacy, and (ii) the right to freedom of expression of the third party expected to disclose the identity of the user. In *Delfi v. Estonia*, the Grand Chamber set out aspects of that case that were relevant to the assessment of whether holding an internet service provider liable for the comments posted by third parties was in breach of freedom of expression. These aspects of *Delfi* also provide a useful guide for balancing the interests in cases where an internet service provider may be compelled to disclose the identity of anonymous users.[54]

26. Firstly, the context and content of the impugned comments must be considered. For example, where the data is being sought in relation to comments that are of a general public interest, then there should be a reduced likelihood that the identity of the user will be disclosed.[55] Secondly, the feasibility of identifying the users of the comments must be taken into account. For example, identification or disclosure may be unduly burdensome or costly for the third party being asked to disclose the identity of the user. Thirdly, courts must consider the measures taken by the third party in explaining to users the circumstances under which a user's identity may be disclosed. For instance, in the Canadian case of *York University v. Bell Canada Enterprises*, the Ontario Superior Court of Justice examined the internet service provider's service agreements and privacy policies when granting an application for a *Norwich Pharmacal* order. The service agreements and privacy

---

49 European Court of Human Rights, *Ürper and Others v. Turkey*, Application Nos. 14526/07 and 8 others (20 October 2009), par. 43; European Court of Human Rights, *Axel Springer SE and RTL Television GmbH v. Germany*, Application No. 51405/12 (21 September 2017), par. 56 and 58.

50 High Court of England and Wales, *Totalise plc v. The Motley Fool Ltd*, [2001] EMLR 750, par. 27; Privy Council, *President of the State of Equatorial Guinea v. Royal Bank of Scotland International*, [2006] UKPC 7, par. 16.

51 Supreme Court of the Netherlands, *Lycos Netherlands B.V/Pessers*, C04/234HR (25 November 2005).

52 Court of Appeal for Ontario, *GEA Group AG v. Ventra Group Co. et al*., 96 O.R. (3d) 481, par. 49.

53 Ontario Superior Court of Justice (Divisional Court), *Warman v. Fournier et al.*, [2010] ONSC 2126, par. 34.

54 European Court of Human Rights, *Delfi AS v. Estonia* [GC], Application No. 64569/09 (2015), par. 144 to 161.

55 See, *Anonymous Online Speakers v. United States District Court for the District of Nevada (In re Anonymous Online Speakers)*, 611 F.3d 653 (2010), par. 18 ("in discovery disputes involving the identity of anonymous speakers, the notion that commercial speech should be afforded less protection than political, religious, or literary speech is hardly a novel principle. [...] The specific circumstances surrounding the speech serve to give context to the balancing exercise.").

policies prohibited the use of the services for posting defamatory material and allowed for identifying information to be disclosed by a court order. The Ontario Superior Court of Justice reasoned that a user could "reasonably contemplate, therefore, that his or her identity may be disclosed by order of the court in the event that he or she engages in unlawful, abusive or tortious activity."[56] Fourthly, courts should also take into account whether the applicant is acting reasonably in seeking the disclosure of the user data. Finally, courts should consider the consequences of identifying the anonymous user for (i) the party seeking disclosure, (ii) the third party disclosing the identity of the user, and (iii) the anonymous user. If the disclosure order is made, the injured party may be able to seek redress for a wrongdoing but, on the other hand, the anonymous user may face negative reprisals.[57] Furthermore, frequent disclosure orders could have a negative impact on freedom of expression online more generally. For instance, internet service providers may institute real name registration to facilitate the disclosure of users' identities. Others may prevent users from commenting on their websites. Some users may be deterred from leaving comments on websites because of the perceived likelihood that they will be identified as the author of those comments.[58] These "negative consequences on the comment environment of an Internet portal" must be considered when deciding whether the disclosure of an anonymous user's identity is necessary and proportionate in a democratic society.[59]

27. In England and Wales, when the courts exercise discretion in making a *Norwich Pharmacal* order, the following aspects of a case are also taken into account to ensure a fair and careful weighing of all the relevant factors;

    1) The strong public interest in allowing an applicant to vindicate his legal rights;[60]
    2) The gravity of the allegations;[61]
    3) Whether the making of the order will deter similar wrongdoing in the future;[62]
    4) Whether the respondent to the application knew or ought to have known that he was facilitating arguable wrongdoing;[63]
    5) Whether the order might reveal the names of innocent persons as well as wrongdoers, and if so whether such innocent persons will suffer any harm as a result;[64]
    6) The degree of confidentiality of the information sought;[65]
    7) The privacy rights of the individuals whose identity is to be disclosed;[66]
    8) The public interest in the confidentiality of journalistic sources;[67] and
    9) Whether innocent third parties can be compensated for their costs.[68]

Media Legal Defence Initiative

---

56 Ontario Superior Court of Justice, *York University v. Bell Canada Enterprises et al.*, 99 O.R. (3d) 695 (9 September 2009), par. 34. See also High Court of England and Wales, *Totalise plc v. The Motley Fool Ltd*, [2001] EMLR 750, par. 27.

57 High Court of Ireland, *Muwema v. Facebook Ireland Ltd (No 2)*, [2017] IEHC 69 (8 February 2017).

58 Delaware Supreme Court, *Doe v. Cahill*, 884 A2d 451 (Del, 2005), p. 457.

59 See European Court of Human Rights, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, Application No. 22947/13 (2 February 2016), par. 86.

60 House of Lords, *British Steel Corpn v Granada Television Ltd*, [1981] AC 1096, p. 1175.

61 High Court of England and Wales, *Totalise plc v. The Motley Fool Ltd*, [2001] EMLR 750, par. 27.

62 House of Lords, *Ashworth Hospital Authority v. MGN Limited*, [2002] 1 WLR 2033, par. 66

63 House of Lords, *X Ltd v. Morgan-Grampian (Publishers) Ltd*, [1991] 1 AC 1, par. 54.

64 High Court of England and Wales, *Alfred Crompton Amusement Machines Ltd v. Customs and Excise Comrs (No 2)*, [1974] AC 405, p. 434

65 Supreme Court of the United Kingdom, *Rugby Football Union v. Viagogo Ltd*, [2012] UKSC 55 (21 November 2012), par. 17.

66 High Court of England and Wales, *Totalise plc v. The Motley Fool Ltd*, [2001] EMLR 750, par. 28.

67 House of Lords, *Ashworth Hospital Authority v. MGN Limited*, [2002] 1 WLR 2033, par. 2.

68 *Id.*, par. 36.